(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2005年5月26日(26.05.2005)

PCT

(10) 国际公布号:
WO 2005/048525 A1

(51) 国际分类号[7]: H04L 9/30

(21) 国际申请号: PCT/CN2004/001289

(22) 国际申请日: 2004年11月12日(12.11.2004)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200310113604.9 2003年11月13日(13.11.2003) CN

(71) 申请人(对除美国以外的所有指定国): 中兴通讯股份有限公司(ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人;及

(75) 发明人/申请人(仅对美国): 丁勇(DING, Yong) [CN/CN]; 陈剑勇(CHEN, Jianyong) [CN/CN]; 彭志威(PENG, Zhiwei) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京同立钧成知识产权代理有限公司 (LEADER PATENT & TRADEMARK FIRM) 中国北京市海淀区花园路13号道隆商务会馆 Beijing 100088 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

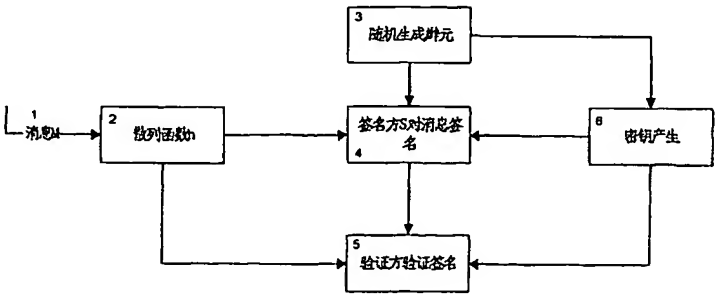
(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO(BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: A DIGITAL SIGNATURE METHOD BASED ON BRAID GROUPS CONJUGACY AND VERIFY METHOD THEREOF

(54) 发明名称: 一种基于辫群共轭的数字签名及其验证方法



1 MESSAGE M
2 HASHING FUNCTION H
3 GENERATE BRAID ELEMENT AT RANDOM
4 SIGNATORY S PUTS SIGNATURE ON MESSAGE
5 SIGNATURE VERIFY PARTY VERIFIES THE SIGNATURE
6 GENERATE PRIVACY KEY

(57) **Abstract:** The present invention discloses a digital signature method based on braid groups conjugacy and a verify method thereof. The signatory S selects three braid elements that $x \in LB_m(1)$, $x' \in B_n(1)$, $a \in B_n(1)$, and considers the braid elements pair (x, x') to be the public key of the signatory S, braid element a to be the private key of the signatory S; signatory S obtains y ($y=h(M) \in B_n(1)$) using hashing function h; generate a braid element $b \in RB_{n-1-m}(1)$ at random, and then put signature on massage M to produce $sign(M)= a^{-1}byba^{-1}$ using its private key a an braid element b generated at random; signature verify party V acquires the public key of S, calculates message M using system parameter hashing function h, and gets y=h(M); determine whether sign(M) and M are conjugate or not, if yes, calculate sign(M)x' and xy using the public key of S which is obtained already and determine whether they're conjugate; if not, sign(M) is the invalid, that's to say, verify fails; if yes, sign(M) is the valid signature for message M. The present invention avoids k-CSP problem in SCSS signature scheme of prior art, increasing the safe degree of signature algorithm, decreasing the number of braid elements used and the times of conjugacy determination in order to improve the calculating efficiency of signature greatly, without reducing the safety.

WO 2005/048525 A1

(57) 摘要

本发明公开了一种基于辫群共轭的数字签名及其验证方法，签名方S选择三个辫元$x \in LB_m(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，将辫元对(x', x)作为签名方S的公钥，辫元a作为签名方S的私钥；签名方S使用散列函数h得到$y=h(M) \in B_n(l)$；随机生成一个辫元$b \in RB_{n-l-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息M签名得到$Sign(M)=a^{-1}byb^{-1}a$；签名验证方V获取S的公钥，利用系统参数散列函数h对消息M进行计算，得到$y=h(M)$；判定$sign(M)$与y是否共轭，若共轭，利用已获取的S的公钥计算$sign(M)$ x' 和xy，并判定二者是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则$sign(M)$为消息M的合法签名。本发明避免了现有技术中SCSS签名体制中的k-CSP问题，提高了签名算法的安全性，在不降低安全性的基础上，减少了参与的辫元的数目和共轭判定的次数，从而大大提高了签名的运算效率。